Court 19

10465066 02

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

STATE OF OKLAHOMA } S.S.
CLEVELAND COUNTY
FILED
APR 20 2020
In the office of the
Court Clerk MARILYN WILLIAMS

LAURA DOUGHTY, individually and on behalf of all similarly situated persons,

Plaintiff,

v.

CENTRALSQUARE TECHNOLOGIES, LLC and CITY OF NORMAN, OKLAHOMA, a municipal corporation,

Defendants.

Case No. CJ-2020-451 TB

CLASS ACTION PETITION

Plaintiff Laura Doughty, on behalf of herself and all similarly situated persons, brings this Petition against Defendant CentralSquare Technologies, LLC ("CentralSquare") and Defendant City of Norman, Oklahoma ("Norman") (collectively, "Defendants"), based on personal knowledge and the investigation of counsel, and alleges the following:

INTRODUCTION

1. This is an action to recover damages from CentralSquare for the harm it caused Plaintiff and a nationwide class of persons whose payment card information was stolen as a result of a data breach on CentralSquare's payment software, Click2Gov. Through this action Plaintiff seeks to obtain refunds for herself and all members of the Norman Subclass, defined below, for fees collected by Norman ostensibly to provide for the security of their payment card transactions.

2. On November 7, 2019, the Norman reported that a data breach occurred on its Click2Gov online utilities payment portal.

Exhibit 1

3. Click2Gov is a payment processing service provided by CentralSquare (formerly known as Superion) and used by municipalities across the United States to collect various payments, including utility bills, parking tickets, taxes, and similar payments.

4. While this is the first known instance of a data breach of the Norman utility payment system, it is far from the first time CentralSquare suffered a payment card data breach. Since mid-2017, hackers have been attracted to CentralSquare's Click2Gov payment portal like flies to a carcass. The first wave of cyber hacks against CentralSquare, which began in 2017 and ended in 2018, resulted in cyber criminals stealing the payment card information of at least 300,000 individuals and selling it to identity thieves on the dark web.[1] The victims were residents of dozens of small-to-medium-sized municipalities across the United States.

5. That's where the story should have ended: in late 2018, with CentralSquare and its municipal clients like Norman so fully on guard against cyber-hackers that nothing like this could happen again. But they weren't, and it did happen again.

6. Beginning in August 2019, a second major data breach on the Click2Gov payment portal took place. Tens of thousands of payment cards and related information, including names, card numbers, expiration dates, and security codes (collectively, "Payment Data"), stolen from individuals who made payments through the Click2Gov portal at dozens of cities, including Norman, has now been sold on black markets on the dark web due to CentralSquare's negligence and Norman's breach of its contractual duty to protect its utility customer's payment card data.

7. Many of these breach victims, including Plaintiff and Class Members, suffered fraudulent charges, had their payment cards canceled, lost use of their funds, lost time contesting

[1]Stas Alforov & Christopher Thomas, *Second Wave of Click2Gov Breaches Hits United States*, GEMINI ADVISORY (Sept. 19, 2019), https://geminiadvisory.io/second-wave-of-click2gov-breaches-hits-united-states/.

Exhibit 1

charges and frantically trying to claw back funds stolen from their bank accounts, driving to and from banks and credit unions, and some have even canceled accounts.

8. Plaintiff brings this action individually and on behalf of Class Members to hold CentralSquare accountable for the harm it has caused and continues to cause to individuals across the country. Norman, and the other municipalities who, like it, charged their utility customers extra fees for payment card security, are required by law and contract to protect customers Payment Data, and when they fail to do so, they should refund those fees for their failure to protect their customers.

PARTIES

9. Plaintiff Laura Doughty is and at all relevant times to this action was a citizen of Oklahoma and a resident of the City of Norman, Cleveland County, Oklahoma.

10. Defendant CentralSquare Technologies, LLC, is a Delaware limited liability company headquartered at 1000 Business Center Dr., Lake Mary, Florida 32746. Upon information and belief, CentralSquare is a citizen of Florida. CentralSquare is licensed to do business in Oklahoma as a foreign limited liability company.

11. CentralSquare is a company whose mission is "To create the broadest, smartest and most agile software platform for building safer, smarter communities."[2]

12. CentralSquare also represents itself as the go-to payment technology provider for public entities:

> A central square is a place where citizens interact with their government, whether it be at city hall, police or fire station, or a hospital. "To square" is designed to communicate taking communities to the next level, and the four corners of a square refer to the four businesses that came together to form CentralSquare. CentralSquare emphasizes putting citizens at the center of everything we offer. We partner with more than 7,500 public sector agencies

[2] "About Us," CentralSquare Technologies, https://www.centralsquare.com/about-us, (last visit on April 14, 2020).

across North America, bringing together two primary drivers for improving people's lives—technology and government"[3]

13. Defendant City of Norman, Oklahoma is an Oklahoma municipal corporation located in Cleveland County, Oklahoma.

JURISDICTION AND VENUE

14. This action arises under the authority vested in this Court by virtue of 12 O.S. §2004(F).

15. Venue is proper in this Court under 12 O.S. §§ 137 and 187, as one of the Defendants, the City of Norman, is a lawful resident in and citizen of Cleveland County, Oklahoma.

16. CentralSquare reached out to Norman to do business in Oklahoma, and a substantial part of the events and/or omissions giving rise to the claims occurred within this State and District.

STATEMENT OF FACTS

A. The Data Breaches

17. As early as the spring of 2017, numerous reports from local news outlets began to report on instances of payment card data breaches that were linked to local utility payment systems. As researchers and reporters honed in, all fingers began to point to one source: CentralSquare's Click2Gov software.[4]

18. In October 2017, CEO Simon Angove of CentralSquare (known at that time as Superion) publicly acknowledged the growing number of data security incidents. He stated:

> Recently we received reports of suspicious activity involving a small number of our customers' computer networks, including possible attempts to steal personally identifiable information. . . . We have notified Superion customers about the suspicious activity and have continued to work closely with the small number of

[3] *Id.*

[4] Stas Alforov, *Dozens of Municipalities Exposed in Click2Gov Software Compromise*, GEMINI ADVISORY (Dec. 18, 2018), https://geminiadvisory.io/hacked-click2gov-exposed-payment-data/.

> affected customers throughout our investigation. As part of our investigation we have identified and notified our customers of certain potential vulnerabilities in the security of their network and provided them with recommendations for addressing the same.[5]

19. CentralSquare's "recommendations" notwithstanding, this "small number of affected customers" proved to be but the nose of the camel.

20. The 2017 and 2018 data breaches started with locally-hosted Click2Gov software systems at individual municipalities, as opposed to cloud-based Click2Gov software hosted directly by CentralSquare.

21. That's where the story should have ended: in late 2018, with CentralSquare and its municipal clients like the City of Norman fully on guard that nothing like it could happen again. But that's not what happened.

22. Beginning in August 2019, a second major data breach on the Click2Gov payment portal took place. The Payment Data of tens of thousands individuals who made payments through the Click2Gov portal at dozens of cities, including Norman, was stolen and sold on black markets on the dark web because of CentralSquare's negligence and Norman's breach of its contractual duty to protect its utility customer's payment card data.

a. The 2019 Breach

23. On November 7, 2019, the City of Norman reported a data breach on its online utilities payment portal (Click2Gov) secured and maintained by CentralSquare.

24. In letters sent to Plaintiff and thousands of other people who used Norman's Click2Gov platform to pay their water bills, Norman stated: "On November 6, the City of Norman received confirmation from their payment vendor that alterations to their software used for online

[5] *CEO Response to Reported Breach*, CENTRALSQUARE, FORMERLY SUPERION (Oct. 13, 2017), available at https://web.archive.org/web/20181202233703/www.superion.com/ceo-response-to-reported-breach/.

Exhibit 1

payments may have enabled unauthorized copying of credit/debit card data. Based on information provided to the City, the 'at risk' dates appear to be between August 26 and October 28[, 2019]." (Hereinafter, the "Breach" or "Data Breach").

25. Thousands of Norman residents had their Payment Data stolen as a result of the Data Breach. And they were not alone.

26. Across the country, city upon city, received the same notice from CentralSquare, and across the country, in city upon city, the utility customers suffered fraudulent charges because of the Data Breach, all caused by the same vulnerability in CentralSquare's Click2Gov program.

27. The dates of the Breach given by CentralSquare to the various cities were largely the same across the country, from August to October of 2019. Over 30 cities were affected by the Data Breach, representing tens of thousands of city residents and utility customers.

28. Because of CentralSquare's specialization in online secure payment processing for public entities, it was on notice of the ever-present and significant threat of Payment Data theft if it did not adequately maintain vigilant and updated security practices. CentralSquare's previous experience with payment card data breaches gave it actual knowledge of these risks and the need to ensure that its IT systems were adequately secured, yet it willfully failed to make the necessary changes to its security practices and protocols, and permitted a massive Data Breach to occur for nearly three months, from August to October 2019.

29. CentralSquare, at all times relevant to this action, had duties to Plaintiff and members of the class to: (a) properly secure Payment Data submitted to or collected at Norman locations and on Norman's internal networks; (b) encrypt Payment Data using industry standard methods; (c) use available technology to defend its systems from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiff and the Class, which would

naturally result from Payment Data theft; and (e) promptly notify customers when Defendants became aware of the potential that customers' Payment Data may have been compromised.

30. As a result of the Breach, many of the victims, including Plaintiff and Class Members, have suffered fraudulent charges, had their payment cards canceled, lost use of their funds, lost time contesting charges and frantically trying to claw back funds stolen from their bank accounts, driving to and from banks and credit unions, and some have even canceled accounts.

31. CentralSquare's failure to adequately protect Plaintiff and Class Members' Payment Data also caused significant additional harms, including the time-consuming requirement to constantly scrutinize bank statements, obtaining and paying for credit monitoring, checking credit reports, contesting false charges, and other efforts that require extensive amounts of time—and often out-of-pocket expenses—while CentralSquare and Norman have done little to nothing to assist the individuals affected by the Data Breach. Defendants have shifted the responsibility for their negligent failures and breaches onto the innocent utilities customers.

32. As a result of the Data Breach, Plaintiff and Class Members suffered actual fraud and losses, including money being stolen from their bank accounts or from their credit accounts, loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payment surcharges made to Norman that Plaintiff and class members would not have made had they known of CentralSquare's negligent approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Payment Data.

B. Industry Standards and Governmental Guidance for Protection of Payment Data

33. Payment card processing companies have issued rules and standards governing the basic measures that merchants and payment software companies, including CentralSquare, must take to ensure that consumers' valuable Payment Data is protected.

34. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires CentralSquare to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

35. The twelve requirements of the PCI DSS are:

a. Install and maintain a firewall configuration to protect cardholder data;

b. Do not use vendor-supplied defaults for system passwords and other security parameters;

c. Protect stored cardholder data;

d. Encrypt transmission of cardholder data across open, public networks;

e. Protect all systems against malware and regularly update anti-virus software or programs;

f. Develop and maintain secure systems and applications;

g. Restrict access to cardholder data by business need to know;

h. Identify and authenticate access to system components;

i. Restrict physical access to cardholder data;

j. Track and monitor all access to network resources and cardholder data;

k. Regularly test security systems and processes; and

l. Maintain a policy that addresses information security for all personnel.[6]

36. Furthermore, PCI DSS sets forth detailed and comprehensive requirements that must be followed to meet each of the twelve mandates.

37. CentralSquare was at all times relevant fully aware of its data protection obligations in light of its participation in the payment card processing networks.

38. CentralSquare was also keenly aware of the risks of payment data breaches because of its prior breaches.

39. Additionally, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 245-47 (3d Cir. 2015); I*n re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005).

40. As long ago as 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses use intrusion detection systems to

[6]Payment Card International (PCI) Data Security Standard, "Requirements and Security Assessment Procedures, Version 3.2.1," (May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1574069601944.

expose a breach as soon as it occurs; monitor all incoming traffic for suspicious activity; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

41. The FTC has issued orders and received judgments against businesses that failed to employ reasonable measures to secure Payment Card Data. The FTC orders provide further notice and direction to businesses regarding their data security obligations. *See, e.g., Wyndham Worldwide Corp.*, 799 F.3d at 245-47; I*n re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465.

42. CentralSquare failed to meet its obligations under the FTC Act and FTC guidance, and failed to comply with the PCI DSS standards.

43. Despite CentralSquare's actual knowledge of the vulnerability of its Click2Gov software, and its actual knowledge that hackers were actively exploiting it, CentralSquare willfully failed to make the necessary changes to its security practices and protocols.

44. CentralSquare's reckless security practices in the face of a known threat permitted hackers to steal the Payment Data of tens of thousands of individuals.

C. The City of Norman Charged Fees for Security It Failed to Provide

45. Businesses are generally not allowed to charge extra fees or surcharges for credit or debit card payments. *See* 14A O.S. § 2-417. There is a limited exception, however, for municipalities. *See* 14A O.S. § 2-211(E).

46. This limited exception for municipalities caps the charge at the actual amount it costs to process the payment card transactions and provide secure payments.

47. Norman charged a $3.00 "convenience fee" for all debit or credit card transactions through the Click2Gov payment program. This fee is intended to assist Norman in paying to

secure its online payment systems.

48. Because of subsection 2-211(E) and the nature of payment card transactions, the security of the transaction was a material part of the agreement between Plaintiff and the Norman subclass and Norman when they paid the $3.00 fee.

49. During the Data Breach, Norman failed to provide this promised security.

50. In effect, therefore, during the time of the Data Breach, Plaintiff and the Norman subclass were paying an additional $3.00 fee for the convenience of giving identity thieves their Payment Data. This is not right.

51. Every convenience fee collected by Norman for payment card transactions through Click2Gov during the Data Breach should be refunded to the Norman subclass.

D. Plaintiff Doughty's Experiences

52. In August, September, and October 2019, Plaintiff Doughty used her debit card to pay her Norman utility bill online through the Click2Gov program.

53. Each time she used Click2Gov she was charged a $3.00 convenience fee.

54. On or around November 21, 2019, Plaintiff discovered that someone had stolen money from her checking account. Between November 13 and 22, 2019, six fraudulent transactions had been made using the debit card that she used to pay her Norman water bill on the Click2Gov software. Altogether, a thief stole over $554.62 from her bank checking account.

55. As soon as she discovered the stolen funds, Plaintiff called her bank and reported the fraudulent transactions. She then called the vendors where the fraudulent payments were made, including a Chick-fil-A, Venmo, Lyft, and PayPal, to see if she could find out more information.

56. Plaintiff contested these transactions with her bank, which canceled her debit card, leaving her without access to her checking account for nearly two weeks. The bank eventually "provisionally" credited the stolen money back to her account while it investigated, but it warned her that it could claw back the money depending on the investigation. For over a month she was left not knowing whether the money would be clawed back or not, limiting her use of her money.

57. On December 10, 2019, Doughty received a letter from the City of Norman notifying her that her debit card was compromised in the Data Breach. She promptly filed a police report with the City of Norman Police Department, notifying them of the fraudulent transactions that had occurred using the same debit card that she used to pay her Norman water bill.

58. Doughty spent over five hours of her time responding to the Data Breach, including contesting the fraudulent charges, requesting a new debit card, filing a police report, and reviewing statements.

CLASS ALLEGATIONS

59. Plaintiff incorporates by reference all allegations in the preceding paragraphs.

60. Plaintiff brings all claims as class claims 12 O.S. § 2023 of the Oklahoma Rules of Civil Procedure. Plaintiff asserts claims on behalf of the following classes (collectively the "Class Members" or the "Class"):

Nationwide Class against CentralSquare (the "Nationwide Class"):

> All persons whose payment card information was compromised in the data breach affecting Central Square Technologies, Inc.'s Click2Gov payment platform occurring between August and October 2019.

City of Norman utilities customers' subclass (the "Norman Subclass"):

> All persons who were charged convenience fees for payment card transactions on the Click2Gov payment portal at the City of Norman, Oklahoma during the 2019 Data Breach.

Exhibit 1

61. Excluded from the Class are Defendant CentralSquare and any entity that CentralSquare has a controlling interest, as well as CentralSquare's officers, directors, legal representatives, successors, subsidiaries, and assigns. Likewise excluded are Defendant Norman, its Mayor, City Council members, and legal representatives. The Class also excludes any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

62. Plaintiff reserves the right to amend the class definition or to seek additional subclasses as necessary.

A. Class Certification is Appropriate

63. The proposed Nationwide Class and Norman Subclass meet the requirements of 12 O.S. § 2023(A) and (B), as required.

64. *Numerosity*: The proposed classes are so numerous that joinder of all members is impracticable. While the total number of individuals affected by the data breach is unknown, based on reporting, the Norman Subclass includes several thousand city utilities customers.[7] The Nationwide Class is much larger, including several thousand residents of each of the over 30 municipalities affected.[8]

65. *Commonality and Predominance*: Common questions of law and fact exist to Plaintiff and all members of the proposed classes. These questions predominate over the questions affecting individual class members. These common legal and factual questions include, but are not limited to, the following:

[7]https://www.koco.com/article/norman-residents-using-online-portal-to-pay-water-bill-could-be-affected-by-data-breach/30200964
[8]https://www.mdjonline.com/news/marietta-utility-customer-data-found-on-dark-web-after-third/article_a233488c-212a-11ea-bc41-ef628c149a23.html

As to CentralSquare and the Nationwide Class:

a. Whether CentralSquare engaged in the wrongful conduct alleged herein;

b. Whether CentralSquare owed a duty to Plaintiff and Class Members to adequately protect their Payment Data, and whether it breached this duty;

c. Whether CentralSquare breached federal and state laws, thereby breaching its duties to Plaintiff and the classes as a result of the Data Breach;

d. Whether CentralSquare knew or should have known that its computer and network systems were vulnerable to attacks from hackers and cyber criminals;

e. Whether CentralSquare's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its computer and network systems resulting in the theft of customers' Payment Data;

f. Whether CentralSquare wrongfully failed to inform Plaintiff and Class Members that it did not maintain computer software and other security procedures and precautions sufficient to reasonably safeguard users' sensitive financial and personal data;

g. Whether Plaintiff and members of the classes suffered injury as a proximate result of CentralSquare's conduct or failure to act;

h. Whether CentralSquare recklessly and willfully violated its duties to Plaintiff and the Nationwide Class; and

i. Whether Plaintiff and the classes are entitled to recover compensatory and punitive damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiff and the classes;

As to the Norman Subclass and CentralSquare:

a. Whether Defendants made representations to Plaintiff and Class Members regarding the privacy and security of their payment cards if used on Defendants' website/payment portal;

b. Whether Defendants' representations created implied contracts;

c. Whether Defendants breached implied contracts to use industry best practices and to comply with FTC guidance to protect Plaintiff and Class Members' Payment Data;

d. Whether Defendants sufficiently addressed, remedied, or protected Plaintiff and Class Members following the Data Breach and took adequate preventative and precautionary measures to ensure Plaintiff and the Class Members will not experience further harm;

e. Whether Defendants' breach of the implied contract and/or the implied covenant of good faith and fair dealing caused Plaintiff and Class Members damages;

f. Whether Plaintiff and members of the Norman Subclass had contracts with the City of Norman that included secure transactions, and whether the City of Norman breached those contracts;

g. Whether Defendants received money from Plaintiff and members of the Norman Subclass to provide for secure transactions;

h. Whether Plaintiff and members of the Norman Subclass failed to receive the security they paid for;

i. Whether it would be unjust for Defendants to retain money received from Plaintiff and members of the Norman Subclass;

j. Whether Plaintiff and members of the Norman Subclass are entitled to reimbursement for money Defendants received from them; and

k. Whether Plaintiff and Class Members are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiff and the classes.

These questions are common to all Class Members' claims and predominate over any and all individual claims that might exist. *See* 12 O.S. § 2023(A)(2) and (B)(3).

66. *Typicality*: Plaintiff's claims are typical of the claims of the classes. Plaintiff and all members of the Nationwide Class were injured through CentralSquare's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other member of the Nationwide Class because Plaintiff and Class Members had their sensitive Payment Data compromised in the same way by the same conduct committed by CentralSquare. *See Id.* § 2023.

Likewise, Plaintiff's claims against City of Norman are typical of the claims of all other Norman utilities users as the event and conduct that gave rise to Plaintiff's claims against Norman are identical to those that give rise to the claims of every other member of the Norman Subclass. Each member of the Norman Subclass had their sensitive PII compromised in the same way by the same conduct of City of Norman. *See Id.*

67. *Adequacy*: Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the class that she seeks to represent; Plaintiff has retained counsel competent and highly experienced in complex litigation and particularly data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action

vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel. *See id.* § 2023(A)(4).

68. *Superiority*: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be difficult if not impossible for members of the Class to individually to effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. *See id.* § 2023(B).

CAUSES OF ACTION

COUNT I - NEGLIGENCE
(Against Defendant CentralSquare Only, on behalf of Nationwide Class)

69. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

70. CentralSquare collected Payment Data from Plaintiff and Class Members in exchange for public utilities payments and other services available online to Plaintiff.

71. CentralSquare owed a duty to Plaintiff and the class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their financial and personal information in CentralSquare's possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing CentralSquare's networks and

data security systems to ensure that Plaintiff's and Class Members' financial and personal information in CentralSquare's possession was adequately protected in the process of collection and following collection while stored on CentralSquare's systems.

72. CentralSquare owed a duty to Plaintiff and Class Members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

73. CentralSquare owed a duty to Plaintiff and Class Members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks—and the personnel responsible for them—adequately protected the financial and personal information of Plaintiff and Class Members whose confidential data CentralSquare obtained and maintained.

74. CentralSquare knew the risks inherent in collecting and storing the financial and personal information of Plaintiff and Nationwide Class members and of the critical importance of providing adequate security for that information.

75. CentralSquare's conduct created a foreseeable risk of harm to Plaintiff and Nationwide Class members. This conduct included but was not limited to CentralSquare's failure to take the steps and opportunities to prevent and stop the Data Breach. CentralSquare's conduct also included its willful decision not to comply with industry standards for the safekeeping and maintenance of the financial and personal information of Plaintiff and Nationwide Class members.

76. As a direct and proximate result of CentralSquare's negligent conduct, Plaintiff and Nationwide Class members have been injured and are entitled to actual damages and punitive damages in amounts to be proven at trial.

COUNT II – NEGLIGENCE PER SE

(Against Defendant CentralSquare Only, on behalf of Nationwide Class)

77. The facts and allegations above are incorporated here by reference.

78. Under the FTC Act, 15 U.S.C. § 45 and its implementing regulations and guidance, CentralSquare had a duty to provide fair and adequate payment systems and conform to certain minimum data security practices to safeguard Plaintiff's and Nationwide Class members' Payment Data.

79. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like CentralSquare of failing to use reasonable measures to protect Payment Data.

80. CentralSquare violated Section 5 of the FTC Act by failing to use reasonable measures to protect Payment Data and not complying with applicable industry standards, including PCI DSS, as described above and incorporated here. CentralSquare's conduct was particularly unfair and unreasonable given the nature and amount of Payment Data it processed and the foreseeable consequences of a data breach, including the immense damages that would result to consumers.

81. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against business who through their failure to employ reasonable data security measures caused the same harm as that suffered by Plaintiff and the Nationwide Class.

82. CentralSquare's failure to comply with the FTC Act by implementing and maintaining reasonable data security measures constitutes negligence *per se*.

83. But for CentralSquare's breach of its duties owed to Plaintiff and the Nationwide Class, they would not have been injured.

84. The injuries suffered by Plaintiff and the Nationwide Class was the reasonably foreseeable (and foreseen) result of CentralSquare's breach of its duties. CentralSquare knew that it was failing to meet its duties and that its breach would cause Plaintiff and the Nationwide Class to suffer the foreseeable harms.

85. Accordingly, Plaintiffs and Class Members are entitled to actual and punitive damages in an amount to be proven at trial, along with the costs and attorney fees incurred in this action.

COUNT III – BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(Against CentralSquare, on behalf of Nationwide Class)

86. The facts and allegations above are incorporated here by reference.

87. CentralSquare entered into a contract with Norman to provide secure payment card processing services for Norman's utilities customers. CentralSquare entered into substantially identical contracts with each of the over 30 cities affected in the 2019 Data Breach.

88. These contracts were made expressly for the benefit of Plaintiff and the Nationwide Class, as it was their Payment Data that CentralSquare agreed to protect.

89. CentralSquare knew that if it were to breach these contracts with the governments the consumers would be harmed, including by fraudulent transactions and related harms.

90. CentralSquare breached its contracts to Norman and the other cities and governments affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach.

91. As foreseen, Plaintiff and the Nationwide Class were harmed by CentralSquare's breach, including fraudulent charges and related injuries.

92. Accordingly, Plaintiff and the Nationwide Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT IV – BREACH OF CONTRACT
(Against the City of Norman, on behalf of the Norman Subclass)

93. The facts and allegations above are incorporated here by reference.

94. Plaintiff and the Norman Subclass used their credit or debit cards to make payments via Norman's Click2Gov payment processing software between August and October 2019.

95. Norman charged Plaintiff and the Norman Subclass a $3.00 convenience fee each time they made a payment during the affected period.

96. This fee included the promise of a secure transaction. Plaintiff and the Norman Subclass therefore had a contract for secure payment transactions.

97. Because Norman failed to provide Plaintiff and the Norman Subclass a secure transaction. Norman therefore breached the contract.

98. Accordingly, Norman owes Plaintiff and the Norman Subclass the fees they paid during the affected period, along with the costs and attorney fees incurred in recovering these fees.

COUNT VI – UNJUST ENRICHMENT
(Against both Defendants, on behalf of the Nationwide Class and the Norman Subclass)

99. The facts and allegations above are incorporated here by reference.

100. This claim is plead in the alternative to the above implied contract claim.

101. Plaintiff and class members conferred a monetary benefit upon Norman in the form of monies paid for the purchase of goods and services from the municipality.

102. Norman appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Norman Subclass members. Norman also benefited from receipt of Plaintiff's and Norman Subclass members' Payment Data, as they was utilized by Norman to facilitate payment to it.

Exhibit 1

103. The convenience fees that Plaintiff and the Norman Subclass paid to Norman were supposed to be used by Norman to pay for the administrative costs of reasonable data privacy and security practices and procedures.

104. Under principals of equity and good conscience, Norman should not be permitted to retain the money belonging to Plaintiff and Norman Subclass because Norman failed to provide the promised security and was in effect charging them money to expose them to identity theft.

105. Norman should be compelled to refund the fees it charged Plaintiff and the Norman Subclass for the use and safety of their electronic payment systems, along with the costs and attorney fees incurred in recovering these fees.

106. CentralSquare, likewise, should disgorge into a common fund for the benefit of Plaintiff and the Nationwide Class members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff Doughty, on behalf of herself and all others similarly situated, respectfully requests that the Court grant the following relief:

a. Certifies a nationwide class against Defendant CentralSquare and a subclass of affected residents in the City of Norman, Oklahoma;

b. Award damages to the Norman Subclass for all convenience fees charged during the breach period, which is a refund of the monthly $3.00 fees that each of the Norman Subclass members paid to City of Norman during the breach period;

c. Award Plaintiff and the Class appropriate monetary relief, including actual damages, punitive damages, restitution, and disgorgement.

d. Award Plaintiff and the class equitable, injunctive and declaratory relief as may be

appropriate; Plaintiff, on behalf of the class, seeks appropriate injunctive relief designed to protect against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information, extend credit monitoring services and similar services to protect against all types of identity theft, especially including card theft and fraudulent card charges;

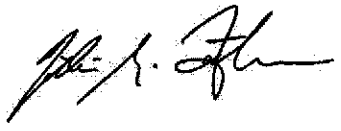
e. Enter an order requiring Defendants to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

f. Enter judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorney fees, costs and expenses as permitted by 12 O.S. § 2023(G); and

g. Any other favorable relief as allowable under law or at equity.

Dated: April 20, 2020

Respectfully Submitted,



William B. Federman, OBA # 2853
Cedric C. M. Bond, OBA # 33119
FEDERMAN & SHERWOOD
10205 N. Pennsylvania
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
ccmb@federmanlaw.com

Attorneys for Plaintiff and the Putative Class

Exhibit 1